# TRAPDOOR ONE-WAY PERMUTATIONS AND MULTIVARIATE POLYNOMIALS BASED ON RANDOM WALKS ON GRAPHS

**M. Klisowski**

Institute of Mathematics, Maria Curie Sklodowska University,
M. Curie-Sklodowska square 5, 20-031, Lublin, Poland
mklisow@hektor.umcs.lublin.pl

Public key cryptography is nowadays commonly used (electronic banking, etc.). Hovever, most of the currently used public key schemes may soon turn out to be completely insecure. As soon as sufficiently large quantum computer is built, most of the problems that are now considered computationally infeasible and are the basis of today's cryptography, will become easy to solve. These problems are integer factorization (the basis of RSA cryptosystem) and discrete logarithm problem (the basis of ElGamal cryptosystem, Diffie-Hellman key exchange and Elliptic Curve Cryptography). For both of these problems there are known efficient quantum algorithms [7,8].

Post-Quantum Cryptography [1] is the domain of Cryptography dealing with cryptographic algorithms that are considered secure against attacks by quantum computers. Multivariate Cryptography [2] is one of the most important directions of Post-Quantum Cryptography. The main idea of Multivariate Cryptography is to use the system of nonlinear polynomial equations as the trapdoor one-way permutations (the most important building blocks of public key cryptosystems). The system should be designed in such a way that solving it (and inverting the permutation) is impossible without some secret information. The problem of solving random system of nonlinear equations is known to be very hard (it is an NP-hard problem).

In papers [9] and [10] V. Ustymenko proposed a family of trapdoor one-way permutations based on the family of graphs of large girth $D(n, q)$. The main idea was to use random walks on these graphs as encryption tools. The vertices of the graph $D(n, q)$ are represented as the sequence of $n$ elements of a finite field $\mathbb{F}_q$. The set of edges is defined by the system of polynomial equations. Consequently, the walk on the chosen path can be represented as a polynomial map $W : \mathbb{F}_q \to \mathbb{F}_q$. This map is further hidden using two invertible affine transformations $A$ and $B$. The public information are the coefficients of the resulting polynomial map $E = B \circ W \circ A$. The secret information (trapdoor) is the walk on the graph and the affine transformations. Some aspects of the computer implementation of this family of permutations was given in [3], [4], [5] and [6].

In this talk we present the orignal construction of the graph based one-way permutation by V. Ustimenko. Next we show that this construction is not secure. We use the fact that the inverse of such permutation is a polynomial map of small degree. We show the way to recover the coefficients of this inverse without the knowledge of secret information by solving properly constructed large system of linear equations.

Finally we present the modification of the original construction. This modification results in a small decrease of efficiency of algorithms (generation of permutations, applying permutations). However the resulting permutation does not have the main defect of the original one — the degree of the inverse polynomial does not have to be small. The degree depends on the chosen finite field and we prove that we can choose a finite field, so that the degree was arbitrarily large.

## References

1. Bernstein D.J., Buchmann J., Dahmen E. *Post-Quantum Cryptography.* Springer, 2009.

2. Ding J., Gower J.E., Schmidt D.S. *Multivariate Public Key Cryptosystems.* Advances in Information Security. Springer, 2006.

3. Klisowski M., Romanczuk U., Ustimenko V. The implementation of cubic public keys based on a new family of algebraic graphs // Annales UMCS, Informatica. 2011. V. 11. No. 2 P. 127–141.

4. Klisowski M., Ustimenko V. On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings // Proceedings of the 2010 International Multiconference on Computer Science and Information Technology (IMCSIT) . 2010. P. 303–308

5. Klisowski M., Ustimenko V. On the implementation of cubic public keys based on algebraic graphs over the finite commutative rings and their symmetries // Albanian Journal of Mathematics. 2011. V. 5. No. 3, P. 139–149.

6. Klisowski M., Ustimenko V. On the comparison of cryptographical properties of two different families of graphs with large cycle indicator // Mathematics in Computer Science. 2012. V. 6. No. 2. P. 181–198.

7. Proos J., Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves // Quantum Information & Computation. 2003. V. 3. No.4. P. 317–344.

8. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. 1997. V. 26. No. 5. P. 1484–1509.

9. Ustimenko V.A. Graphs with special arcs and cryptography // Acta Applicandae Mathematicae. 2002. V. 74. No. 2. P. 117–153.

10. Ustimenko V.A. Maximality of affine group, and hidden graph cryptosystems // Algebra Discrete Math.. 2005. No. 1. P. 133–150.